risk of identity theft:

- Remain vigilant, especially over the next 12 months, and review your bank accounts, credit card bills and free credit reports for unauthorized activity. Promptly report any suspected identity theft to your local law enforcement agency, the U.S. Federal Trade Commission, your State Attorney General, your financial institution, and to the Fraud Alert phone line of a consumer reporting agency. You can obtain information about fraud alerts and security freezes by contacting one of the three national reporting agencies below:

B142581

cps

P.O. Box 989728
West Sacramento, CA 95798-9728

Jodie Pierce
[redacted]

Enrollment Code: VF7MPLYZP2
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/cps-matter

April 9, 2025

Notice of Data Breach

Dear Jodie Pierce,

CPS Solutions, LLC ("CPS Solutions"), which helps support pharmacy operations, is writing to inform you of a recent cybersecurity incident that may have affected your personal information. CPS Solutions works with many hospitals and health care providers to help patients receive medications at a reduced cost or for free. This event may have involved your data.

What Happened:
On December 4, 2024, CPS Solutions discovered that an unauthorized third party gained access to one CPS Solutions employee's O365 business email account. Upon discovery, CPS Solutions immediately forced a password reset, disabled the email account, and took other appropriate steps to prevent further access. The email account was secured that same day and an investigation was launched to determine the potential scope and impact. Our findings indicate that an unauthorized third-party was able to access and remove data from the account, which may have contained limited personal information, between December 2 to 4, 2024. On January 24, 2025, CPS Solutions completed a comprehensive review which identified all customers and individuals potentially affected by this incident and what information was involved. Based on the results of that review, we formally notified your health care provider of this incident on February 10, 2025.

What Information was Involved:
The personal information involved may have included: (1) full name, date of birth, and address; (2) health insurance information (such as member/group ID number or Medicaid/Medicare number); and/or (3) medical information (such as medical record number, clinical information, provider information, diagnosis or treatment information, or prescription information such as medication name). Not all data elements were involved for every potentially affected individual.

For the majority of potentially affected individuals, Social Security numbers were not impacted. Driver's license numbers, credit and debit card information, bank account information, test results, images, and hospital medical records were also not involved in this incident.

What We Are Doing:
CPS Solutions takes privacy and security seriously. As soon as the incident was discovered, we took immediate action to mitigate and remediate the incident and to help prevent further unauthorized activity. In response to this incident, security and monitoring capabilities are being enhanced and systems are being hardened as appropriate to minimize the risk of similar incidents in the future.